Referentia Systems Incorporated

Final Scientific Report
General Distribution Version

ONR Contract N000-06-C-0107, CDRL A002-2

Pacific Missile Range Facility (PMRF) Force Protection Lab Phase I

Concept Exploration for Navy Facility Open Access Technology and Processes

Compiled by:
David C. Brauer, Program Manager, Referentia

Submitted to:
Office of Naval Research
875 North Randolph St.
Attn: David Masters Code: 03D&I
Arlington, Virginia 22203-1995

Team Members:

Referentia	SAIC
Vic Askman	Stephen Hennessy
Jim Chatigny	Stephen Karwoski
Adam Forsyth	Roger Medd
Jim Hino	Max Tsai
Matthew Shawver	David Turner
Stephen Upton	Chris Warner
James Wang	

Document Number: RSI-PFPL-A002-v1.0
Date: April 30, 2005

SAIC
An Employee-Owned Company

REPORT DOCUMENTATION PAGE, SF 298

REPORT DOCUMENTATION PAGE — *Form Approved OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*	30-04-2006
2. REPORT TYPE	Final Scientific Report
3. DATES COVERED *(From - To)*	23-12-2005 - 30-04-2006
4. TITLE AND SUBTITLE	Final Scientific Report, General Distribution Version, Pacific Missile Range Facility (PMRF) Force Protection Lab Phase I Concept Exploration for Navy Facility Open Access Technology and Processes
5a. CONTRACT NUMBER	N000-06-C-0107
5b. GRANT NUMBER	
5c. PROGRAM ELEMENT NUMBER	CDRL A000-2
5d. PROJECT NUMBER	
5e. TASK NUMBER	
5f. WORK UNIT NUMBER	
6. AUTHOR(S)	Referentia Program Manager: David C. Brauer Referentia Team: Vic Askman, Jim Chatigny, Adam Forsyth, Jim Hino, Matthew Shawver, Stephen Upton, James Wang SAIC Program Manager: Stephen Karwoski SAIC Team: Stephen Hennessy, Roger Medd, Max Tsai, David Turner, Chris Warner
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	Referentia Systems Incorporated 550 Paiea Street, Suite 236 Honolulu, HI 96819-1837
8. PERFORMING ORGANIZATION REPORT NUMBER	RSI-PFPL-A002-v1.0
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	Office of Naval Research Code: 03D&I 875 North Randolph St. Arlington, Virginia 22203-1995
10. SPONSOR/MONITOR'S ACRONYM(S)	ONR
11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT	Distribution limited to U.S. Federal Government agencies and authorized bidders for PMRF Force Protection Lab Phase II. Other requests for this document shall be referred to ONR/03D&I.
13. SUPPLEMENTARY NOTES	

14. ABSTRACT

This final scientific report presents the methodology, assumptions and procedures used to conduct the 4 month PMRF Force Protection Lab (PFPL) Phase I "Concept Exploration for Navy Facility Open Access Technology and Processes" research activity. The basis of this work included: The PMRF Base Survey, the Scenarios, Behaviors, Observables and Measures of Effectiveness document, and the Security Technology Survey. Building on this foundation, the PFPL Security Benchmarking Tool (PFPL-SBT) was developed leveraging agent-based modeling and simulation technologies and data farming. The PBPL-SBT was used to conduct effects analysis and cost-benefit analysis of PMRF and potential security solutions. A Baseline Architecture, prioritized effects and recommended investment priorities for future work are presented.

15. SUBJECT TERMS

Open-access base security, sensor/security technology effects, agent-based modeling, data farming

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	19b. TELEPHONE NUMBER *(Include area code)*
Unclassified	Unclassified	Unclassified	SAR		David C. Brauer	(808)423-1900 x161

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The long term goal of the Pacific Missile Range Facility (PMRF) Base Protection Lab (PBPL) is to establish a new paradigm for open-access military base security. This Final Report summarizes the results of the 4 month PMRF Force Protection Lab (PFPL) Phase I "Concept Exploration for Navy Facility Open Access Technology and Processes" conducted by Referentia Systems Incorporated and its subcontractor, SAIC.

The report presents the methodology, assumptions and procedures used to conduct this research and development activity. The basis of this work was a technology survey activity which yielded three supporting documents: The PMRF Base Survey, the Scenarios, Behaviors, Observables and Measures of Effectiveness document, and the Security Technology Survey. Building on this foundation, the PFPL Security Benchmarking Tool (PFPL-SBT) was developed leveraging agent-based modeling and simulation technologies and data farming. The PBPL-SBT was used to conduct effects analysis and cost-benefit analysis of PMRF and potential security solutions.

A Baseline Architecture for the PBPL Phase II was developed building upon the results of the effects analysis and the technology survey. The architecture presents a concept for the testbed that goes beyond sensor integration and situational awareness displays to create a "cognitive architecture" supporting reasoning and learning about normal/abnormal behaviors and potential threats.

The results and discussion section of this report presents four key baseline effects that should guide the phase II efforts. These are:

1. *Pre-event and historical information are required to establish the context for reasoning and learning.*
2. *Observed behaviors need to be associated with a time and location.*
3. *Primary behaviors, behaviors that are directly threatening, need prior contextual information.*
4. *Secondary and tertiary behaviors should be correlated to lead to a conclusion of malicious intent.*

The PFPL-SBT tool provides a fully implemented cost-benefits analysis feature. Given the time and data available to this phase I effort, a rigorous cost-benefits analysis could not be completed. However, the following recommendations were generated regarding investment priorities for PBPL Phase II

- *Development of a cognitive software architecture that establishes a context for reasoning and learning.*
- *Development of standardized notations and ontologies for communicating about tracks, behaviors, hypotheses, beliefs and intent.*
- *Intelligent agents implementing multiple techniques to reason about behaviors and threats and "learn" normal base activity.*
- *Algorithms/reasoning to determine observed behaviors from raw and fused sensor data.*
- *Algorithms/reasoning to determine malicious intent from observed behaviors.*

1. INTRODUCTION

1.1 BACKGROUND

The long term goal of the Pacific Missile Range Facility (PMRF) Force Protection Lab (PFPL) is to establish a new paradigm for open-access military base security. Prior to 9/11, many military bases offered fairly open access to beaches, lakes, trails and other recreational areas to the public. In addition, military bases often played host to special events that were open to the public. Since 9/11, security concerns have severely limited use of military areas for public use and in some cases this has created a hardship on the surrounding civilian population and adverse public relations.

In recent years, with increased focus on homeland security and force protection for deployed troops, significant security technology advances have been made that will allow relatively open access while ensuring a safe and secure environment for military bases and preserving the capability to achieve their missions. The PFPL will be a testbed research and development facility for implementing, testing and evaluating technologies to:

- Discriminate normal activity from unusual patterns of behavior
- Detect precursor behaviors predictive of threat activities
- Help the security force anticipate, respond and interdict threats before they impact missions or cause harm
- Reduce overall cost and manpower while preserving desired level of access and security

The PFPL will draw upon a variety of promising security technologies such as:

- Advanced sensors (positional ID/RFID, chem-bio-nuclear trace detection, high-resolution electro-optic/infrared cameras)
- Sensor fusion processing (e.g. multi-hypothesis tracking, information fusion, automated correlation)
- Feature extraction (video analytics, pattern recognition, neural networks, Bayesian networks)
- Human behavior recognition (facial recognition, deceptive behavior, determination of intent)
- Situational awareness (GIS and 3-D visualization, multi-layer alerts, indicators and warnings, decision aids)
- Data mining (historical trending, predictive analysis, learning)
- Knowledge management (process/scenario models, concept model, descriptive model, reasoning, uncertainty management)

1.2 PURPOSE AND SCOPE

The purpose if this phase 1 effort is to define the problem space and range of research and development foci for PFPL Phase II. The purpose of the PFPL Phase II is to provide a realistic testbed environment where promising security technologies can be developed, integrated, tested and evaluated to determine high-performing, cost-effective, “best of breed” solutions. The PFPL will leverage the wide diversity of PMRF facilities and geography to present representative security challenges. To avoid impacting critical base missions or assets, non-critical facilities and base locales will be used as proxies for test and evaluation purposes.

The PFPL is not intended to be a new security system for PMRF and direct integration with existing base security systems would not only compromise the R&D function of the PFPL testbed, but could potentially have an adverse impact on existing security. Over time, tested, best-of-breed security technology solutions will be transitioned from the PFPL to PMRF base security.

The primary outcome of the research and development conducted at PFPL will be new solutions for open-access base security leveraging emerging, state-of-the-art technology in advanced sensors, situational awareness, behavioral analysis, and other R&D efforts. It is envisioned that PFPL will position PMRF at the leading edge of open-access base security R&D, testing and evaluation.

1.3 INTENDED AUDIENCE

Referentia's Final Scientific Report for the Pacific Missile Range Facility (PMRF) Force Protection Lab PFPL Phase I "Concept Exploration for Navy Facility Open Access Technology and Processes" is only intended for use with the PMRF Base Protection Lab (PBPL) Phase II Broad Agency Announcement (BAA). Distribution is limited to U.S. Federal Government agencies and authorized bidders for PBPL Phase II. Other requests for this document shall be referred to ONR/03D&I.

The methodology, results and software described in this report are intended to provide a framework for the development of PBPL Phase II proposals. Phase II bidders are not required to adhere to this framework or to use the associated software. Each bidder may propose what they consider to be the best solution(s) to the challenges presented in the Phase II BAA. This report and the associated software tools are not to be used for any other purpose but the preparation of Phase II proposals.

This report, appendices and associated software are unclassified. Portions of the supporting documentation and software have been redacted to protect potentially sensitive information.

2. METHODS, ASSUMPTIONS AND PROCEDURES

2.1 TECHNOLOGY SURVEY

2.1.1 Base Survey

Representatives of the Referentia PFPL team visited Pacific Missile Range Facility (PMRF) Kauai, Hawaii from 9 January to 13 January 2006. The team met with base security, facilities and operations personnel to discuss their current security challenges and concerns. Base personnel also provided an extensive tour of base facilities. The team observed normal base operations and gained an understanding of the normal flow of activities. These observations provided a good foundation for ongoing modeling efforts. The security subject matter experts (SMEs) on the Referentia team documented the base survey from a risk assessment and vulnerability perspective (see appendix 5.1).

The most significant result of the Base Survey visit was that the team gained a clear understanding of the wide range of base security issues that can be "staged" at PMRF. With proper design and management, the PFPL Testbed can be used to test solutions for a variety of security challenges without affecting the primary mission and operations of PMRF. Notional assets can be configured to represent:

- *Operations Facilities*
- *R&D Facilities*
- *Mission/Test Facilities*
- *Airfields/Flight Lines*
- *Communications Resources*
- *Radar/Sensor Installations*
- *Ammunition Storage*
- *Fuel Storage*
- *Troop/Crew Quarters*
- *Military Housing*
- *Guest Housing*
- *Schools/Child-Care*
- *Entertainment/Sports Facilities*
- *Water Supplies*
- *Power Plants*
- *Port Facilities*

PMRF is relatively remote and isolated and has normal and peak staffing levels that represent a reasonable test case for behavioral analysis and threat analysis R&D. The base presents a wide range of geographic features including: ocean/beachfront access on its western border, farm fields and undeveloped areas on its eastern border, a sparsely developed area to its south, and an undeveloped area to its north. Outlying facilities extend to mountainous terrain, sea cliffs and beachfront/waterfront terrain. Considering the range of facilities and geographies along with the manageable sample size, PMRF represents an ideal location for a base security testbed.

2.1.2 Scenarios, Behaviors, Observables and Measures of Effectiveness

Building upon the results of the Base Survey, the security SMEs developed four primary notional threat scenarios to illustrate event activities, observables, and human activity associated with an event. These scenarios included:

- *Scenario 1: A vehicle-borne explosive device (VB-ED) and Hostage Situation*
- *Scenario 2: Suicide Bomber at Community Event*
- *Scenario 3: Insider Theft of Classified Information during Facility Operations Center peak operations*
- *Scenario 4: A Coordinated Vandalism and Event Disruption activity*
- *Note: An additional scenario was developed concerning stealthy incursion for explosive device or chemical/biological device (ED/CB) placement.*

The Scenarios, Behaviors, Observables and MOEs (SBOM) document is provided in appendix 5.2. Each scenario provides a detailed timeline of pre-event, during event and post-event activities, behaviors and observables along with a notional geographic layout of the event. This level of detail is sufficient to develop realistic threat scenarios in the PFPL Security Benchmarking Tool (see section 2.2.1). For the phase I baseline effects analysis, the 4 primary scenarios were used to provide comparable benchmarks for different possible security solutions resulting in a prioritized set of effects (observables and behaviors) that should be addressed by the security solutions developed in the PFPL testbed. The requirements table provided at the end of the SBOM document was used to create the canonical set of behaviors and observables emitted by agents in the PFPL-SBT tool.

2.1.3 Security Technology Survey

Since 9/11, a vast amount of effort and funding as been directed to research, develop and deploy new facilities protection technology. This rapidly growing technology sector has become too large to adequately survey in the 4 months allocated to this phase I effort. To scope this effort, the requirements generated by the Scenarios, Behaviors, Observables and MOEs guided the technology analysis. The following seven categories of technology were reviewed:

- **Land Barriers with Contact/Proximity Sensing**
  - Fences or other barriers that are instrumented to detect tampering

- **Low-Profile Incursion Detection Systems**
  - Systems that can detect and characterize (to some level) activity along a perimeter or within an area. No barriers are used, and these may be visible or concealed. Included here are:
    - Permanently installed perimeter incursion devices using buried coax or fiber optic cable
    - Permanently installed or emplaceable non-imaging perimeter or area incursion devices (microwave, infrared, acoustic, seismic, or multi-sensor combinations)
    - Combinations of non-imaging and imaging systems (video or still imagery) that are actively monitored and controlled to detect and visually characterize events.

- **Badge, Portal, and Tracking Systems**
  - ID badge (contact, proximity, or RF-based) and associated reader/monitoring systems capable of monitoring, allowing and recording access to specific portals or

movement throughout an area. This section also included physical portal or barrier devices that can be opened or deployed based on badge readings

- **Biometric Authentication for Point Access**
  - Fingerprint, iris or face recognition systems used to defeat identity deception

- **Explosives Detection Systems**

- **Nuclear, Chemical, Biological Sensors**
  - Specialized systems, usually deployed at portals, to detect explosive traces or NBC signatures

- **Water, Underwater Incursion Detection and Barrier Systems**
  - Acoustic, imaging or other systems designed to detect incursion (boats, swimmers, divers) from off shore.

Measures of effectiveness (MOEs) and measures of performance (MOPs) were developed for each of these categories. The PFPL Technology Survey (appendix 5.3) includes 1-2 representative systems from each category and a rough order of magnitude (ROM) cost estimate for each. The ROM estimates for some of the representative systems were entered into the PFPL-SBT tool to support cost-benefit analysis.

2.2 BASELINE MODEL

2.2.1 PMRF Force Protection Lab Security Benchmarking Tool (PFPL-SBT)

The primary focus of the phase I effort was the development of a computational model to conduct effects analysis of the implementation of candidate access and security technologies. Per ONR BAA 05-016, “The intent is not to model specific sensors or approaches but the effect of the capability in satisfying access and security objectives; i.e. effect of detecting all movement and activity on base; effect of identifying all moving objects on base; effect of reducing the timeline of detection and identification; and other contractor defined effects.” Referentia leveraged its experience on Project Albert (Marin Corps Warfighting Lab contract #M00264-03-C-007) and applied agent-based distillation models to create a modeling and simulation environment for effects analysis of threat scenarios and security solutions. Figure 1 shows the main user interface for the PMRF Force Protection Lab Security Benchmarking Tool (PFPL-SBT).

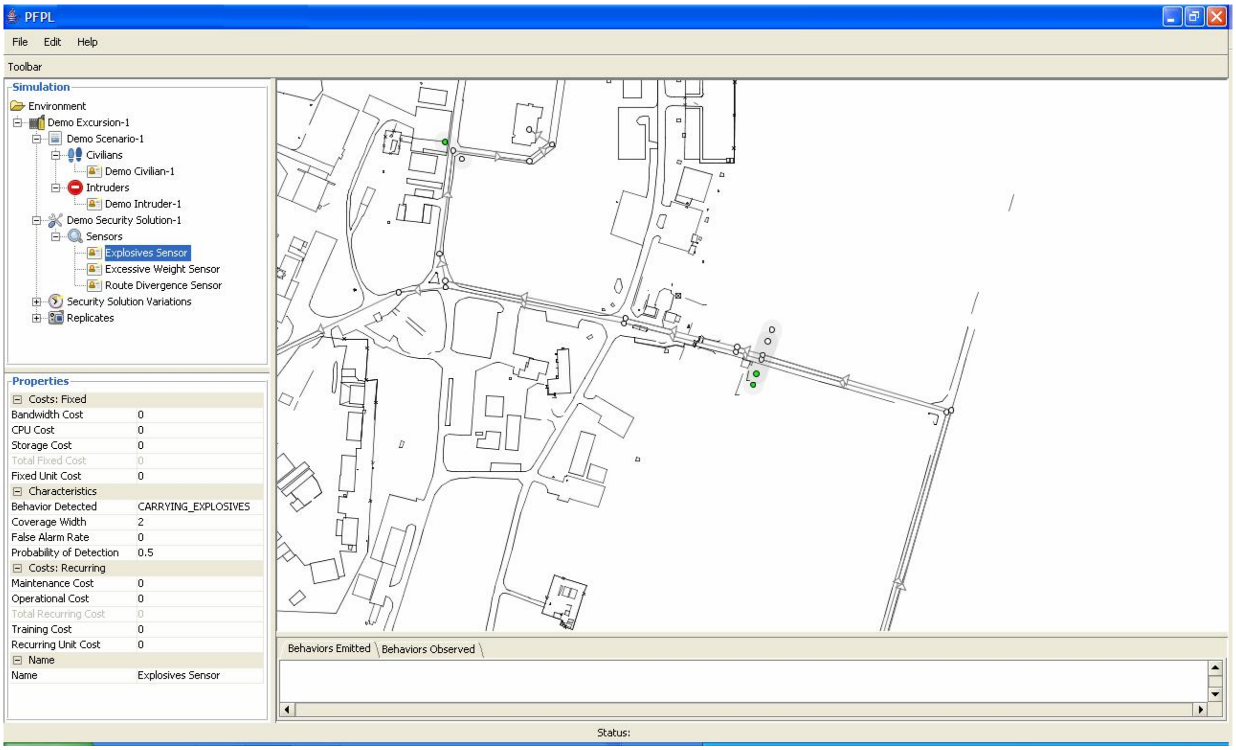


Figure 1: PFPL-SBT Main User Interface

The PFPL-SBT is a tool that allows security specialists and technologists (including sensor designers, developers of security operating procedures, behavior recognition algorithm researchers, etc.) to gain insight into the applicability of proposed solutions to base security problems. The tool focuses on behavior and the ability to detect and recognize it. It allows users to define notional scenarios where actors (simulation agents) emit specific behaviors, and then notional solutions which are intended to identify those behaviors which are “abnormal” in the context of the scenario. The solution can then be run against the scenario using the agent-based simulation engine which underlies the SBT. Analyzing the results of these runs can aid the user in evaluating the suitability of the proposed solution for the scenario.

As shown in Figure 1, the base buildings, roads, boundaries and facilities are represented by a simple 2D map in vector format which allows the user to zoom out to view the entire base or zoom all the way in to a single building. For this version of the tookl, PMRF facilities have been obfuscated to avoid compromising base security.

In the model, agents represent moving objects (people, vehicles, etc.) and security technologies (sensors) placed on the map. Agents emulate the behavior or effect of the objects they represent. Scenarios are scripted movements of non-threat (civilian) and threat (intruder) agents around and on the base. These agents emit observable behaviors.

Security Solutions are layouts of security technologies (sensors) that can detect certain observable behaviors within a specified coverage area with a specific probability of detection and false alarm rate.

An Excursion is a 1-1 combination of a specific scenario and a specific security solution. A Replicant is an executable simulation of an excursion with a specific random number seed. When a replicant is run, a log is generated of all of the behaviors emitted by agents as they move across the base. Another log is generated of behaviors detected by sensors based upon their coverage area, probability of detection and the random seed.

A data distribution can be generated for an excursion using variations on the security solution and multiple replicants. This can provide insight into the efficacy of the security solution for the given scenario. By using the same security solution in multiple excursions (e.g. paired with a variety of different scenarios) it is possible to gain insight into the overall performance of a security solution. By using the same set of scenarios as a benchmark over a number of possible security solutions, it is possible to compare the efficacy and cost of the solutions.

The PFPL-SBT also leverages the Project Albert concept of Data Farming. By using a technique know as “Design of Experiments”, analysts can pick which parameters to obtain coverage of the potential problem space. This can reduce the number of data distributions which must be generated from millions to thousands or even hundreds. The batch mode of PFPL-SBT can then be used to set up the parameters and to run a large number of variations and replicants on the excursions of interest. The built in graphing tools of PFPL-SBT can be used to plot measures of effectiveness across a number of scenarios to look for trends or the data set can be exported and analyzed in external tools such as MatLab. Cost factors can also be plotted.

Figure 2 shows one example of an analysis performed by running variations of sensor false alarm rates (FAR) against variations of probability of detection (PD). Its not surprising to find a peak in the number of correctly identified intruders when we have a relatively high FAR, because we would also be having a high number of false positives. What is interesting in this example is that we achieve the same level of true positives at the lowest FAR when we set the PD at around 0.7. Figure 3 shows the same data for true positives on civilians and also shows a good level of performance with the lowest FAR and a PD around 0.7. So for this particular sensor solution, development goals should focus on a very low FAR and a moderate PD.

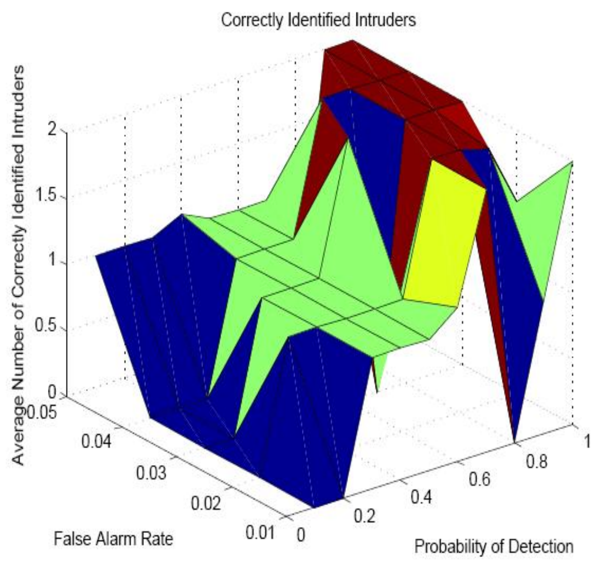


Figure 2: True Positives for Intruders

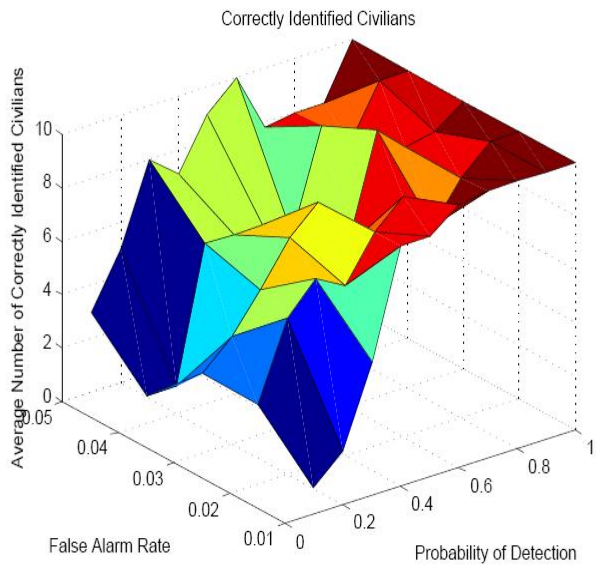


Figure 3: True Positives for Civilians

2.2.2 Effects Analysis

Effects analysis using the PFPL-SBT Tool focused on answering the question, "If we had a sensor or security technology that had the EFFECT of detecting X, what would be the impact within our benchmark treat scenarios?" The baseline analysis for effects was performed context-free, that is without any location specific or geography specific information and enabled the assignment of the basic set of behaviors (from the SBOM document) into four distinct categories:

Primary Behaviors are behaviors that are directly threatening. They lead to an immediate conclusion of malicious intent without requiring any prior context. The primary behaviors encoded in the PFPL-SBT model include:

- TAMPERING_WITH_OBJECT
- DAMAGING_DETROYING_OBJECT
- DISCARDING_ETAG
- DIVERGING_FROM_ROUTE
- CARRYING_WEAPON
- CARRYING_FIREARM
- INITIATING_FALSE_ALARM
- ATTEMPTING_UNAUTHORISED_ENTRY
- MAKING_UNAUTHORIZED_ENTRY
- SETTING_FIRE_TO_OBJECT
- BREACHING_FENCE
- FAMILIAR_HOSTILE
- CARRYING_EXPLOSIVES
- CARRYING_WMD

Secondary Behaviors are behaviors that may not necessarily be directly threatening, but tend to lend strong evidence to a conclusion of malicious intent. They may provide context for primary behaviors or may be combined with other secondary and tertiary behaviors to lead to a conclusion that threatening behavior is apparent. The secondary behaviors in the PFPL-SBT model include:

- MOVING_ERRATICALLY
- VEHICLE_SPEEDING
- MOVING_EXCESSIVELY_FAST
- VICINITY_RESTRICTED_OBJECT
- CARRYING_STOLEN_ID
- VEHICLE_EXCESSIVELY_HEAVY
- INITIATING_FALSE_ALARM
- OPENING_UNLOCKED_DOOR
- DIVERGING_FROM_ROUTE

Tertiary Behaviors are behaviors that are weakly indicative of malicious intent. These behaviors do not generally indicate intent directly. However, these behaviors can add weight to a conclusion of malicious intent when combined with secondary behaviors. It is not likely that a combination of tertiary behaviors can be used to determine intent. The tertiary behaviors in the PFPL-SBT model include:

- RUNNING
- LOITERING
- CIRCLING
- MOVING_BACK_AND_FORTH
- VICINITY_LOCKED_DOOR
- BEHAVING_NERVOUSLY
- AVOIDING_PORTAL
- UNUSUAL_ARRIVAL_TIME
- APPROACHING_FENCE
- VICINITY_FENCE
- VICINITY_PORTAL
- APPROACHING_PORTAL
- ENTERING_PORTAL
- OPERATING_RENTAL_VEHICLE
- UNFAMILIAR_PERSON

Quaternary behaviors are behaviors that do not indicate intent. These behaviors rarely help determine intent, and do not contribute to the prior probabilities when combined with secondary or tertiary behaviors. An example might include “walking.” While these behaviors do not seem to be worth monitoring, it might be instructive to consider that the absence of these behaviors may point to anomalous behaviors. These behaviors may be good indicators of the day-to-day “normal” activity of the base. The quaternary behaviors in the PFPL-SBT model include:

- PRESENT
- ALONE
- IN_GROUP
- WALKING
- DRIVING
- STATIONARY
- STOP_MOVING
- START_MOVING
- JOINING_GROUP
- LEAVING_GROUP
- ATTAINED_GOAL
- CARRYING_PASS
- CARRING_OTHER_ID

- CARRYING_ETAG

After context-free effects analysis was performed and the 4 levels of behaviors were defined, data farming techniques were used across the 4 primary scenarios against several notional sensor and security technology solutions. Recommendations resulting from effects analysis are presented in section 3.1.

2.2.3 Cost-Benefit Analysis

The PFPL-SBT tool was designed to support comparative cost-benefit analysis of sensor/security technology solutions. Each solution element can be assigned the following cost factors:

- Fixed Costs: Unit Cost, Bandwidth, CPU, Storage (Total is calculated)
- Recurring Costs: Recurring Unit Cost, Maintenance, Operational, Training (Total is calculated)

The intent for cost-benefit analysis was to create exemplary sensor/security technology solutions based upon the Security Technology Survey (appendix 5.3). These exemplars would then be paired with the primary scenarios to create multiple excursions. By plotting the excursions using the cost factors as MOEs, it should have been possible to determine an “investment balance” between sensors, bandwidth, CPU, storage and other factors. Unfortunately, the Security Technology Survey did not contain sufficient detail on cost factors to support this comparison. However, through the development of the PBPL-SBT and the Baseline Architecture (presented in section 2.3), the Referentia team was able to develop a set of recommended investment priorities. These are presented in section 3.2.

2.3 Baseline Architecture

Referentia's recommended baseline architecture for the PFPL testbed is presented in Figure 4. The baseline architecture was motivated to a large extent by the architecture needed to support the PFPL-SBT model. In particular, we found that the model required a rudimentary "cognitive architecture" incorporating a simple rule-based architecture in order to support effects analysis of primary, secondary and tertiary behaviors. The Scenarios, Behaviors, Observables and MOEs document as well as the Security Technology Survey also provided key information for the formulation of the baseline architecture. Inputs to the architecture come from sensors via a common sensor interface and data fusion as well as external databases providing contextual information. The Data and Knowledge Repository are tightly coupled and could even be implemented within a common database. Ontologies representing the relationships between data, tracks, hypotheses and beliefs are used to map data into knowledge to support reasoning. The cognitive architecture provides the two major functions of behavior recognition and threat analysis. Intelligent agents are recommended for implementing these functions to allow for the simultaneous execution of multiple approaches to reasoning and learning. The primary output of the architecture is the situational awareness display which displays alerts, warnings, tracks and security assets and guides response control. This display will allow the user to zoom-in on particular elements to view raw data feeds and/or historical data. The data collaboration function exports and redacts (where necessary) data and knowledge from the repository and makes it available as a Web service to remote researchers.

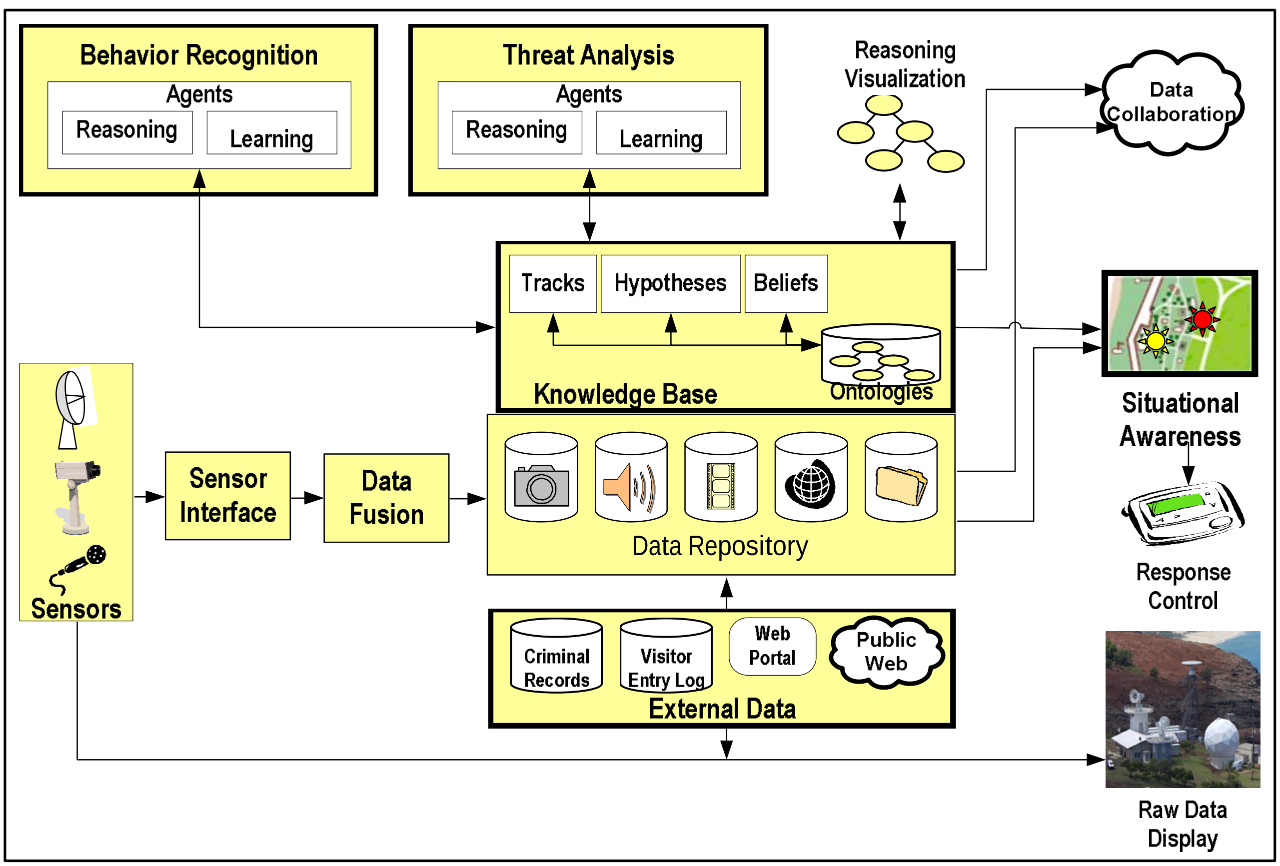


Figure 4: PFPL Testbed Baseline Architecture

2.3.1 Baseline Architecture Use Cases

The primary use case for the baseline architecture follows:

- The system gathers information about the prevailing state of affairs.
    - Sensors continuously monitor different areas of the base.
    - Agents periodically access external data sources over the network.
    - A Web site accepts inputs from humans.
- An operator monitors the state of affairs on a situational awareness display. The situational awareness display is a geographic rendering of the area. The rendering includes static objects such as buildings as well as detected objects of interest such as people and vehicles. Detected objects are displayed in real-time. The operator has the ability to zoom into areas of interest.
- Information gathered by the system is fused into a common set of tracks. In other words, different information referring to the same object is fused to form a single object instance.
- Behaviors are formulated by analyzing the fused tracks.
- Over time, the system learns what sort of behaviors are to be expected.
- Threat analysis is performed by comparing the currently observed behaviors with the sorts of behaviors that are expected. The threat analysis may request other data from local or remote databases to better determine the state of affairs.
- Unexpected behaviors create an alert to the operator. The alert includes a threat level and a location of the alert on the situational awareness display. Alert thresholds will be able to be adjusted for normal activity versus during an exercise or visit by a dignitary
- The operator can review information leading up to the reported alert. The information may be a single event or a series of events. The information presented will include the time, date and location of the event. The operator will be able to drill down into all available information including threat level, snapshots and resolution logs.
- The operator indicates to the system whether or not the alert is warranted.
    - If the alert is not warranted, the system may ask the operator to input additional information so that it can learn more about the situation.
    - If the alert is warranted, the system may suggest an investigative course of action based on the current state of security assets.
- Following each investigative action, a description of what was done and the outcomes are entered into the system to support subsequent analysis.

The PFPL project is an R&D effort. It is therefore important to consider the use cases for the development phases of the project as follows:

    - The development of the system will be executed by a number of contractors working on different functional areas such as sensors, behavior recognition, displays and threat analysis.

- Researchers view the architecture as the framework through which they can effectively contribute to the construction of a semi-autonomous system that improves itself with experience.
- Developers use the architecture to identify framework components that are of practical importance to their implementations, and to design appropriate extensions, additions or other modifications.
- Contractors may be developing the identical functional capability with different approaches that need to be evaluated.
- Various configurations of sensors and functional components must be easily constructed, integrated and tested.
- Spiral builds will be released on at least an annual basis.
- Experimentation information will be shared with researchers on and off site.

2.3.2 Architecture Top Level Requirements

- The architecture shall be modular. It is expected that multiple contractors will be developing parts of the system in parallel. Functional partitioning of the system into functional modules with well-defined interfaces shall be essential to the realization of this requirement.
- The architecture shall be extensible. The addition of sensors and algorithms over time requires extensibility not only in the addition of new sensors but also recognition of diverse behaviors that may be unforeseen in the initial development. New algorithms to process these behaviors will also be developed over time.
- The architecture shall support experimentation. The architecture must support a rapid prototyping environment where configurations of sensors and algorithms can be rapidly generated and evaluated. The architecture also needs to support testing for integration and evaluation.
- The architecture shall be real-time. A continuous flow of new information must be processed without significant backlog. The latency requirements are those imposed by human reaction time (seconds).

2.3.3 Baseline Architecture Details

2.3.3.1 Sensors

Sensor information shall take the form of raw data such as video or shall be processed information that may provide information such as the position of an object of interest.

2.3.3.2 Sensor Interface

The sensors feed the system through a common sensor interface that merges all sensor input into a common data stream. This interface will allow seamless incorporation of sensor suites.

2.3.3.3 Data Fusion

The data fusion function shall take information from the various sources and associate them to form tracks. These tracks will form the basis of monitoring all objects within the system. Data fusion at the earliest stages of detection allows the same object detected by different sensors to be associated with a single track. Data from external sources will also be associated to tracks by the data fusion function.

2.3.3.4 External Data

External data comes primarily from available databases such as visitor entry logs or sources outside of the base such as criminal record databases. External data may also be entered by the operator or through a Web site (e.g. an event reported wirelessly by a guard). External data may be continuously updated or may be requested when required.

2.3.3.5 Data Repository

The data repository shall maintain a cache of the recent history for processing as well as long term history for display. Client functions shall have the ability to update information in the cache and request notification when information is changed. The amount of history stored in the data repository shall be a function of a specified maximum time as well as the constraints of the storage media.

2.3.3.6 Knowledge Base

The architecture shall support the use of ontologies by maintaining descriptions of their properties, interrelationships and conditions under which they are appropriate. Like other types of software, the ontologies will evolve as the system matures. Initially an upper ontology will be developed for the project domain that overarches a family of lower metaphorical ontologies. Relationships spanning lower ontological concepts will be defined to support collective reasoning among agents that employ different viewpoints. As new approaches to implementing reasoning are introduced, or additional useful viewpoints are derived, the ontology catalog will be expanded accordingly.

2.3.3.7 Behavior Recognition

The behavior recognition function shall train itself through continuous track observation. It will reason about the observed properties of tracked objects in the context of knowledge it has already acquired regarding normal base activities. The behavior recognition function shall be comprised of a collection of functions that reason cooperatively form different viewpoints. Over time, these functions will develop an understanding of routine base activities and learn to expect certain types of behaviors to be observed in certain places at certain times. Deviations from these expectations form the basis of threat assessments. Behavior interpretations will be made available to operators in a form that they can easily understand.

2.3.3.8 Threat Analysis

The threat analysis function shall monitor recognized behaviors associated with tracks over time. Tracks that are unable to be associated with recognized behaviors, or that are associated with unexpected behaviors, shall be considered to be an indication of a potentially threatening incident. Individual incidents may not warrant attention but a series of events over a period of days or months may be an indication of an impending undesirable event. An impending undesirable event will generates an operator alert. The threshold of alerts shall be based upon a parameter set by the operator.

2.3.3.9 Agents for Reasoning and Learning

The behavior recognition and threat analysis functions shall be comprised of reasoning agents. The software architecture shall accommodate various approaches to implementing learning and reasoning, and shall provide suitable hypothesis and belief spaces within the data repository for reasoning agents to share. Tracks, hypotheses and beliefs will be associable such that queries can return elements from one or all categories.

2.3.3.10 Reasoning Visualization

Reasoning visualization allows for an operator to investigate the chain of reasoning which led to a particular conclusion. It also supports human-directed learning where operators “teach” the system when something is normal and when it is not.

2.3.3.11 Situational Awareness

The situational awareness function shall provide the operator with views of the current and historical state of the monitored areas. The operator shall have the ability to visualize all activity in the monitored area and zoom into areas of interest. This function shall also provide the alerts of impending undesirable events. The operator indication shall take the form of a DEFCON level from 1 to 5 as well as alerts to specific events of interest.

2.3.3.12 Response Control

The response control function shall monitor the state of the security assets such as patrols. The response to the action shall be saved with the event to for subsequent use by the behavior recognition function. Action response information will help teach the system how to better interpret behaviors in the context of future conditions on the base.

2.3.3.13 Raw Data Display

The display of raw data is extracted into its own module to allow the process to be replicated and distributed across multiple processors.

2.3.3.14 Data Collaboration

The data collaboration function shall archive experimental results and post the results to be shared by researchers. The data shall be in both machine and human readable forms. The information shall include data collected as a part of the run as well as text and graphics that analyze the performance results. The data collaboration module extracts experimentation data, formats the data and posts the data on private portal accessible over the Internet.

3. Results and Discussion

3.1 Baseline Effects

Effects Analysis using the PFPL-SBT tool as well as design of experiments and data farming led the Referentia team to four key conclusions regarding prioritized effects.

1. Pre-event and historical information are required to establish the context for reasoning and learning. Information such as schedules, activities and normal usage patterns on base as well as reinforced (learned) relationships between observable behaviors create a knowledge-base of what is "normal" on the base. This can be compared with current data to help establish conclusions about abnormal behavior and behaviors indicative of malicious intent. External database are also necessary to collect this pre-event and historical information such as:
   - Law enforcement, base security, good Samaritan and other HUMINT
   - Communications intercepts and other SIGINT around base

   Examples of potentially significant pre-event information include:
   - Arrival/Settlement of potential hostile in area
   - Potential hostile seeking employment on base
   - Signs of insider cooperation with external agents
   - Information gathering about operations and vulnerabilities by external agents
2. Observed behaviors need to be associated with a time and location. Surprisingly, much of the security technology currently fielded does not provide precise tagging of events with both time and location. Alarms may be tripped without an associated time stamp. Video capture might have a time association, but location may not be precise. Associating all data with a common detail level of time and location facilitates data fusion, track formation and associated reasoning. Time and location information enriches historical information and supports learning.

   Examples of information with critical time/location features include:
   - Detection of a person in an "overwatch" position
   - Detection of movement across base perimeter
   - Unauthorized entry to secured area
3. Primary behaviors, behaviors that are directly threatening, need prior contextual information. Although primary behaviors lead to an immediate conclusion of malicious intent, they tend to happen too late in an event timeline for a meaningful security response. Because of their immediacy, primary behaviors are the focus of most available security technology.

   Examples of primary behaviors that benefit from contextual information include:
   - Breaching fence or other perimeter demarcation
   - Carrying a weapon or explosive without authorization

- Attempting unauthorized entry
- Initiating a false alarm

4. Secondary and tertiary behaviors should be correlated to lead to a conclusion of malicious intent. This will require the development of algorithms and/or reasoning to correlate these behaviors. Because these behaviors happen early in the event timeline, they can provide valuable early warning to security forces of potential threats.

   Examples of secondary behaviors include:

   - Speeding vehicle
   - Moving towards or in the vicinity of restricted area

   Examples of tertiary behaviors include:

   - Diverging from and authorized route
   - Arriving at an unusual time

3.2 RECOMMENDED INVESTMENT PRIORITIES

The development of a cognitive software architecture that establishes a context for reasoning and learning is crucial to successful research and development in PBPL Phase II. To achieve the vision of a new paradigm for base security, significant research advances will be required. Although there have been significant advances in security technology since 9/11, understanding of the base security situation remains a cognitive process in the minds of experienced security guards. By developing a cognitive software architecture, multiple techniques can be investigated for enabling the computer to understand what is normal and what might represent a potential threat.

The development of standardized notations and ontologies for communicating about tracks, behaviors, hypotheses, beliefs and intent is needed to realize the cognitive architecture. There currently exists no common meta-language for different security technologies (sensors, cameras, ID tags, data fusion, video analytics, etc.) to communicate and share information. The development of this common language in PBPL Phase II would benefit not only the testbed, but the security technology industry as a whole.

Intelligent agents should be used to implement multiple techniques to reason about behaviors and threats and to "learn" normal base activity. This will enable multiple researchers to participate in developing the two core functions of the cognitive architecture: behavior recognition and threat analysis. It will also allow multiple techniques to be compared or to be composed into a cooperative architecture.

Algorithms and reasoning techniques to determine observed behaviors from raw and fused sensor data need to be developed. These should present their hypotheses and beliefs about tracks and potential malicious intent in the common meta-language.

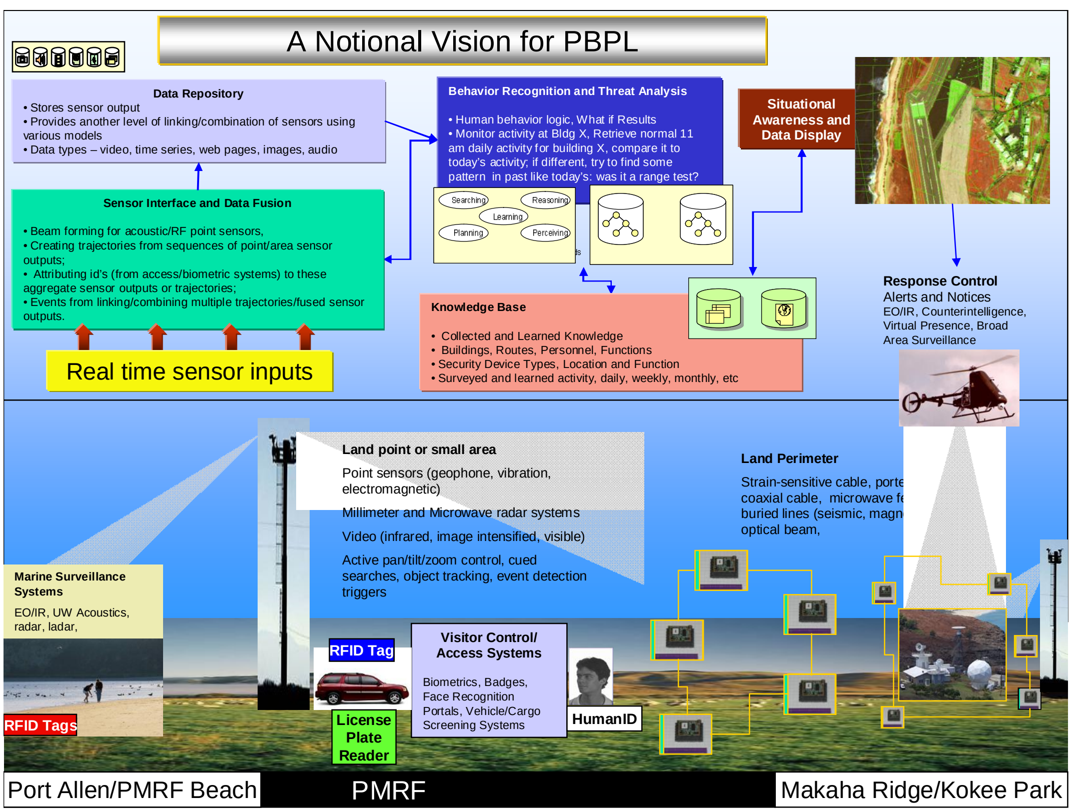
Algorithms and reasoning techniques to determine malicious intent from observed behaviors are the ultimate outcome of the PBPL Phase II effort. These will enable the system to understand the current base situation and to warn security forces about potential malicious activities in time for a meaningful response.

4. CONCLUSIONS

The four-month PFPL Phase I effort, "Concept Exploration for Navy Facility Open Access Technology and Processes," conducted by Referentia and its subcontractor, SAIC, yielded significant results to support the successful execution of the PMRF Base Protection Lab (PBPL) Phase II initiative. This Final Technical Report, the PFPL-SBT Modeling and Simulation Tool and Referentia's Industry Day Presentation provide all competitors for the Phase II effort with a level playing field:

- The background information of the Base Survey provides a common understanding of the current security issues and challenges at PMRF and illustrates how the base can be used to stage a variety of assets for security test and evaluation.
- The Scenarios, Behaviors, Observables and MOEs document provides a benchmark set of threat scenarios that potential Phase II partners can use to test their security solution concepts.
- The Security Technology Survey provides an initial set of technologies to investigate.
- The PMRF Force Protection Lab Security Benchmarking Tool (PFPL-SBT) provides a sophisticated agent-based modeling and simulation environment for building treat scenarios and security solutions. The integrated data farming and analysis tools allow for thousands of comparative runs for testing a proposed solution.
- The Baseline Architecture provides a one clear, fully conceived vision of how the phase II testbed could be implemented.

Figure 5 presents one possible vision for the PBPL testbed.



5. APPENDICES

5.1 PMRF BASE SURVEY

5.2 SCENARIOS, BEHAVIORS, OBSERVABLES AND MEASURES OF EFFECTIVENESS

5.3 SECURITY TECHNOLOGY SURVEY

5.4 PFPL-SBT USER'S GUIDE